AU/ACSC/SIMMONS/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Operationalizing Cyberspace for Today's Combat Air Force

by

Travolis A. Simmons, Major, United States Air Force

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Colonel (ret) Richard M. Perry

Maxwell Air Force Base, Alabama

April 2010

Distribution A: Approved for public release; distribution unlimited

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Figures

Acknowledgements

I would like to express my sincere appreciation to my primary faculty advisor, Mr. Richard “Kemo” Perry, for his patience and guidance throughout this project. Additionally, I could not have completed this journey without the technical expertise provided by Mr. Roger Philipsek, Lieutenant Colonel Mark “Chappie” Smith, Lieutenant Colonel J. T. Thill, Major Marc Flores, and Major Ann Halle. Thank you for graciously entertaining the numerous requests, questions and brainstorming sessions.

I would be remiss if I did not offer thanks to Dr. Dan Kuehl, Mr. Fred Green, Lieutenant Colonel William “BH” Poe, Major Joseph “Mule” Koslov, and the cyber professionals at JFCC NW, JTF-GNO, STRATCOM, PACOM, and CENTCOM. Thank you for the education you provided. Your knowledge was invaluable to the successful completion of this project.

Finally, I would like to thank my family for your love and support throughout this demanding project and always.

Abstract

This study researches the question, "*What does the CAF operator need to know about CNO?*" Section 1 provides the framework for the discussion as well as key background information regarding current United States Government strategic views and DOD views on cyberspace. Section 2 begins the CNO education by showing where CNO fits into the overarching information operations construct and concludes by providing a generic discussion of the interaction between each of the elements.

Section 3 furthers the discussion by detailing how cyber forces are organized. Section 4 outlines the importance of CNO to the warfighter. Section 4 also lends vulnerability and capability analysis in an effort to drive the CAF mission planner or operator to think in terms of desired effects. Section 5 highlights a few of the key operational challenges in the areas of doctrine, organizational thought and system architecture, education and training, and planning in order to highlight issues that may hamper CNO support to the warfighter.

The author concludes that *it is vital for the CAF operator to have working knowledge of CNO – organization, importance, and challenges* – in an effort to facilitate better integration into the warfighting structure. This study provides that knowledge while also offering recommendations to promote more efficient joint cross-domain operations.

Section 1: Introduction

Due to rapid technological advancements levied by the information age, the United States is now more reliant than ever on networks and information systems. From telecommunications and banking to transportation and infrastructure, networks are pervasive throughout all aspects of American life. Whether it be the Federal Aviation Administration servers that enable control of the nation's air traffic or the Supervisory Control and Data Acquisition (SCADA) systems that enable control of critical infrastructure such as electric grids, water, and sewer treatment, networks and information systems are fundamental to most normal daily activities. The critical component that enables the all-important transfer of data between information systems across networks is the domain of cyberspace. Cyberspace affects virtually every aspect of society.

Developing a globally acceptable definition for cyberspace is no simple task. In fact, there are almost as many definitions for cyberspace as there are methods for operating within cyberspace. While continual evolution of technology will likely demand future refinement, currently, Dr. Daniel T. Kuehl, professor at National Defense University, takes the best components of current thought on the matter and offers the most comprehensive definition. He states, "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technology."[1]

As far back as 2003, the White House recognized the importance of cyberspace when calling it the country's "nervous system".[2] Furthermore, the current administration has devoted vast resources to cyberspace security. Shortly after inauguration, President Obama ordered a top-down review of cyber security. After receiving the results of that 60-day review, the President

declared, "Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."[3] Additionally, the findings also led to the establishment of a new office at the White House to be led by the Cyberspace Coordinator. While cyberspace is clearly fundamental to the daily operation of the nation's industrial base, it is also vital to effective operations within the Department of Defense (DOD). Globally, DOD operates more than "15,000 computer networks" and "seven million computers" daily to support normal functions as well as warfighting efforts.[4] The inherent value of the cyberspace domain is that it enables not only the operation within, but also the domination of the four other domains of land, sea, air and space. The 2010 Quadrennial Defense Review Report (QDR) offers,

> There is no exaggerating our dependence on DOD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.[5]

Considering the current economic turmoil within the United States and the resultant reduction in Department of Defense budgets and personnel, it is vital that leadership properly structure and integrate operations within the domain of cyberspace. Furthermore, it is of equal importance that the CAF warfighter be operationally familiar with what cyberspace professionals bring to the fight, their capabilities as well as their vulnerabilities, in order to properly and efficiently plan, execute, and win current and future conflicts. While there are several important questions that remain unanswered with regard to cyberspace, the task of this document is to focus primarily on the integration of computer network operations (CNO). This research will provide the CAF operator with working knowledge of CNO – organization, importance, and

challenges – in an effort to facilitate better integration into the warfighting structure. Furthermore, the author will offer recommendations to promote more efficient joint cross-domain operations.

Section 2: What is Computer Network Operations

Joint Publication (JP) 1-02 defines cyberspace operations as, "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid [GIG]."[6] Mention of the GIG requires subsequent mention of a supporting concept – network operations (NetOps). DODI 8410.02 defines NetOps as "[t]he DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG. NetOps includes, but is not limited to, enterprise management, net assurance, and content management."[7] It is impossible to discuss CNO without first identifying NetOps as a critical enabler to CNO. In order to conduct CNO, one must first have a network in which to operate. If cyberspace operations were an iceberg, then NetOps would be the 90% of the iceberg that is below the surface, while CNO is the 10% above sea level. To comprehend CNO fully, one must also understand where it fits into the warfighting spectrum. At the highest level, information operations provide the umbrella that covers CNO. JP 3-13 defines information operations as "the integrated employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOPs), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own."[8] EW and CNO are unique in that they have the ability to accomplish all of the defined tasks.

Due to the sensitive nature and classification levels of CNO, the discussion rendered within this research will remain broad and generic. CNO is comprised of three separate divisions: Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND). CNE is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[9] Stated simply, CNE is the infiltration of networks or systems to gain intelligence or to prepare the battlespace for CNA. One of the many unanswered questions with regard to cyberspace is "*what constitutes an attack?"* There are very few laws created specifically for cyberspace issues. One of the main problems with the lack of cyber law is that one nation's exploitation effort could be interpreted as an attack by the target nation. Furthermore, in the absence of law, should morality, proportionality, or both govern the response? Many of these issues paint the fine line that exists between CNE and CNA.

CNA, which can be loosely associated with offensive counterair/counterspace, is an action used to manipulate or destroy information located on a system or network or the system/networks themselves. By definition, the task of CNA is to "disrupt, deny, degrade or destroy."[10] CNA is an inherently difficult task due to the extreme intelligence requirement in order to execute a single operation. Leigh Armistead, author of *Information Operations* states, "the intelligence needed to conduct a computer network attack is an order of magnitude greater than what may be needed for a bombing mission."[11] In addition to the vast intelligence requirement, the rapidly changing nature of information systems presents another challenge for CNA. Even after accomplishing the many tasks required to plan and develop a CNA, the attack is one system patch, software update, or security breech away from failure. In short, what works

today, may not work tomorrow; this fact feeds back to the vast intelligence effort required for successful CNA.

CND, which can similarly be linked to defensive counterair/counterspace, is "actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks."[12] CND synthesizes adversary threat analysis with friendly vulnerabilities to provide software and hardware countermeasures for employment in order to protect the GIG from external as well as internal threats.

Figure 1 below shows a generic CNO diagram. This figure is notional in nature and does not depict any DOD capabilities or processes. The arrow in the middle of the figure represents a random network. The bottom third of the figure shows CNA tasks, whereas the top third details CND tasks. While the figure clearly depicts the integration of CNE throughout the CNA process, the importance of CNE in CND is not clear. CND requires a vast amount of intelligence, much of which is gained through CNE, in order to properly analyze the threat and to effectively secure friendly systems. Figure 1 also highlights another point about legal authorizations to execute CNO: Although United States Code Title 10, Title 18, and Title 50 are shown on the CND side of the chart, their implications span CNO. While execution under Title 18 (law enforcement – i.e. FBI, DEA, etc.) is straightforward, execution of Title 10 (Armed Forces) and Title 50 (War and National Defense) present unique challenges for cyberspace operators. Title 50 personnel are typically different from Title 10 personnel. Title 50 authorizes CNE, while Title 10 authorizes CNA and CND. With the requirement for close integration, the challenge is to determine *who executes specific tasks* and *when execution occurs during an operation*. Answers to these questions are critical in a time-sensitive environment where microseconds define the difference

between success and failure. Close integration is so important that the United States Air Force Space Command (AFSPC) identified it as one of the primary risks to successful operation of the 24th Air Force by stating, "If cyberspace-unique United States Code (USC) Title 10 and USC Title 50 relationships are not more fully defined in rules of engagement, transient high value targets may be missed. Intelligence professionals performing SIGINT activities often cannot share information with operators in an actionable timeframe."[13]

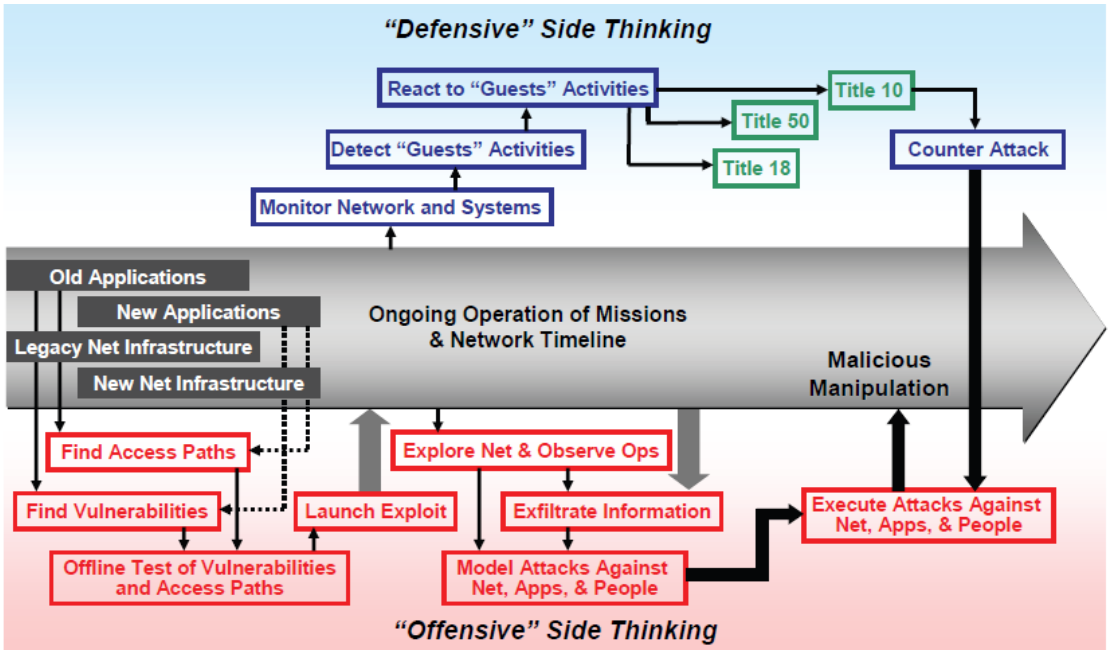


Figure 1 Generic CNA/CND Diagram[14]

Section 3: Organization

With regard to organization, United States Strategic Command (USSTRATCOM) is the combatant command responsible for cyberspace operations. In addition to tasking USSTRATCOM as the central synchronizer for planning cyberspace operations within and external to DOD, the Unified Command Plan (UCP) details USSTRATCOM's responsibilities as follows.

1. Directing GIG operations and defense
2. Planning against designated cyberspace threats

3. Coordinating with other CCDRs and appropriate US government agencies prior to the generation of cyberspace effects that cross areas of responsibility
4. Providing military representation to US national agencies, US commercial entities, and international agencies for matters related to cyberspace, as directed
5. Advocating for cyberspace capabilities
6. Integrating theater security cooperation activities, deployments, and capabilities that support cyberspace operations, in coordination with the geographic combatant commanders, and making priority recommendations to the Secretary
7. Planning operational preparation of the environment (OPE), and as directed, executing OPE or synchronizing execution of OPE in coordination with geographic combatant commanders
8. Executing cyberspace operations, as directed[15]

These cyber responsibilities currently reside with two USSTRATCOM functional components: Joint Functional Component Command-Network Warfare (JFCC-NW) and Joint Task Force-Global Network Operations (JTF-GNO). JFCC-NW is co-located with the NSA. The commander of JFCC-NW serves a dual role as Director of NSA (DIRNSA). JFCC-NW's mission, primarily offensive in nature, is to "assure allied freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain".[16] Similarly, JTF-GNO is located with the Defense Information Systems Agency (DISA). Likewise, the commander of JTF-GNO is also the Director of DISA (DIRDISA). JTF-GNO's mission is to "direct operation and defense of the GIG to assure timely and secure Net-Centric capabilities across strategic, operational, and tactical boundaries in support of Department of Defense full spectrum warfighting, intelligence, and business missions."[17]

While all services present forces to USSTRATCOM to assist in the mission of conducting CNO, we will focus primarily on Air Force presentation of the 24th Air Force. When discussing the Air Force CNO, it is important to note a slight deviation from the joint terminology. What JP 3-13 calls CNE, CNA, and CND, Air Force Doctrine Document (AFDD) 2-5 terms network exploitation (Net-E), network attack (Net-A), and network defense (Net-D). Essentially, the terms are interchangeable. As shown in Figure 2, the cyber forces presented to

JFCC-NW and JTF-GNO come from the 67th Network Warfare Wing and the 688th Information Operations Wing. The operators reside primarily in the 67th NWW. Operator training and engineering infrastructure are two of the many support functions owned by the 688th IOW. A critical relationship not depicted in Figure 2 is that between USSTRATCOM and the Air Force Intelligence Surveillance Reconnaissance Agency (AFISRA). As the Service Cryptologic Component (SCC), AFIRSA has oversight of all of the CNE within the Air Force, even that which is embedded within the 24th AF.[18]

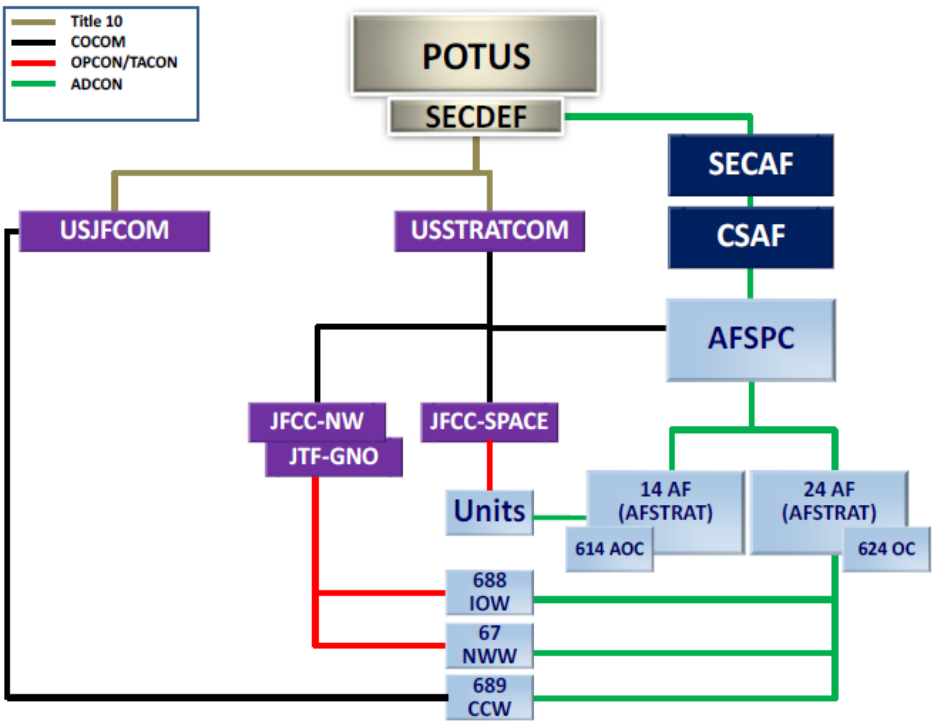


Figure 2 USAF Force Presentation to USSTRATCOM[19]

On 23 June 2009, Secretary of Defense Robert Gates released a memorandum directing the establishment of United States Cyber Command (USCYBERCOM), a USSTRATCOM sub-unified command, to direct DOD operations in cyberspace. USCYBERCOM will absorb the resources and responsibilities of JFCC-NW and JTF-GNO as well as the association with NSA and DISA. This guidance requires disestablishment of JFCC-NW and JTF-GNO and full

operating capability (FOC) of USCYBERCOM no later than October 2010.[20] One of the greatest benefits to establishing USCYBERCOM is the synergistic effect created by having all aspects of the cyber force co-located. Deputy Secretary of Defense William J. Lynn III stated, "Combining offensive and defensive capabilities under a single roof and bringing those together with the intelligence we need to anticipate attacks will make our cyber operations more effective." [21]

Section 4: Importance to the CAF Operator

Vulnerabilities

It is practically impossible to overemphasize the DOD's reliance on networks. Figure 3 below shows just a few of the many DOD uses. A close examination of Figure 3 reveals numerous essential systems that are required for daily operations. Most of the conveniences provided by networks have become so common that they are now transparent to the casual observer. That transparency remains intact until the network ceases to function normally and daily tasks are halted. General Kevin P. Chilton offered, "You can have perfect logistics, perfect maintenance, best trained crews in the world – you can be shut down if you don't have your networks."[22] Recognition of this dependency is important because it leads to the realization that the same dependency invites exploitation through the security vulnerabilities inherent within the networks. Stated simply, adversaries attempt to exploit networks because users are so dependent upon networks. Therefore, safeguarding known vulnerabilities is paramount.

According to the SANS (SysAdmin, Audit, Network, Security) Institute, most vulnerabilities fall within three primary categories. They are network vulnerabilities, operating system (OS) vulnerabilities, and application vulnerabilities. [23] Network vulnerabilities consist of weaknesses in the coding that operates network hardware. In order to exploit these vulnerabilities, attackers must know the types of hardware that comprise the network.

Exploitable hardware includes routers, switches, servers, intrusion detection systems (IDS), and intrusion prevention systems (IPS). OS vulnerabilities are exploitable weaknesses in the code that controls the user interface. Common OS's include Windows 7, Windows Vista, Windows XP, Mac OS X, and Linux. Until recently, OS vulnerabilities were the category most targeted by attackers. The new leader however, is application vulnerabilities.[24] One reason application vulnerabilities are so popular is because of the sheer number of applications available. Widely used applications such as the Microsoft Office package and Adobe products are prime examples of heavily targeted programs. Additionally, patches for application vulnerabilities become available at a much slower rate than OS patches, which leaves systems open to exploitation for longer periods. Attackers also target applications through the practice of turning trusted web sites into malicious servers. These servers consistently target browsers as well as applications that can be manipulated via browsers.[25] The threat of exploitation by malicious servers is one of the many reasons why DOD prohibits access to certain websites and prohibits the use of unapproved applications.

Vulnerability Implications

Although most CAF operators will likely not be responsible for updating router firmware or installing OS patches, it remains vital that everyone recognize and understand the current threat. Many of DOD's key tactical networks are closed or "air-gapped" networks. They include primary warfighting systems such as Link-16, Intra-Flight Data Link (IFDL), and other critical command and control networks. While air-gapped networks are more difficult to penetrate because they lack a direct internet connection, they are subject to compromise through human error and are therefore not impenetrable.[26] While the author agrees with the vulnerability categories as stated by the SANS institute, one key intangible that must not be omitted is the

human element. Dr. Kuehl stated, "The way that people do things can defeat the technological measures of security."[27] Each time an individual sits in front of a computer, he/she must be cognizant of the responsibility to protect friendly networks.

There are many means by which the previously mentioned vulnerabilities may be exploited. Having to execute a major combat operation without the use of key networks is one of the more alarming outcomes of such exploitation. While it would be quite challenging to operate in the absence of key networks; likewise, imagine the panic that would ensue if the networks were operating but the transmitted information was not trustworthy. The results could certainly prove deadly for some fighter aircraft that rely on networks for identification purposes. In short, the likely implication of severely compromised networks during combat is total chaos, and that is best case.

IP-based Communication Networks - Internet - NIPRNet, SIPRNet, etc. - Voice Over IP (VOIP) Telephony Systems - Banking Infrastructure	Closed-network Battlefield Systems - Integrated Air Defense Systems (IADS) - Tactical Data Information Links (TADIL) - C^2 Networks
Distributed Control Systems - Supervisory Control and Data Acquisition/Control Systems (SCADA/CS) - Manufacturing Process Control Systems - Energy Generation and Distribution Systems	Tactical Communication Networks - Theater Airborne and Terrestrial Radio Systems - Mobile Radios (cell phones, mobile data services) - Land Mobile Radio (LMR) (first responder, law enforcement, local C2 networks)
Transportation Control Systems - Regional or Global Air Traffic Control (ATC) Systems - Airfield Air Traffic Control and Landing Systems (ATCALS)	Global Communications Networks - Satellite Communications Networks (SATCOM) - Fiber Optic Networks - Telephony - Global Positioning Systems

Figure 3 Example Networks in Cyberspace[28]

Capabilities

Since all U.S. specific capabilities are highly classified, this section will cover a few generic exploitation and attack tools commonly used by current international cyber players, state and non-state actors alike. Again, this discussion will *not* detail U.S. systems or tactics. The most commonly used cyber tools are viruses, worms, Trojan horses, blended threats, botnets and denial of service (DoS) attacks. Viruses, worms, Trojans horses, and blended threats all fall under the MALicious softWARE or *malware* umbrella. The baseline malware weapon in the cyber attacker's arsenal is the virus. A virus is "a computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission."[29] The critical distinction within that definition is the fact that a virus, much like a parasite, requires a vehicle to propagate itself. A virus is not a self-contained entity capable of movement in the absence of a host file. The 1999 *Melissa* virus became one of the more widely known and widespread viruses of its time. The virus infected Microsoft Word documents and spread itself by emailing infected documents to the first 50 contacts in the Microsoft Outlook address book. Even machines that did not operate Outlook retained the potential to spread the virus via Word documents saved on floppy disks. Although *Melissa* did not destroy, delete, or steal data, it "exploited one of the most valuable benefits of the net – the ability to share documents – to propagate and to multiply itself, it affected more people and spread faster than earlier viruses."[30]

A more malicious cyber tool is the worm. "Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network."[31] One of the important qualities of worms is that they often use large amounts of memory as they replicate

on an infected system. The replication can result in a system that is overloaded and unable to function at normal speeds. Many of the most commonly known computer viruses such as *I love you* and *Slammer* were actually not viruses at all, but were, in fact, worms. One of the most sophisticated worms created to date is the 2008 *Conficker* worm. Although there is little agreement among experts, estimates of the number of computers infected range as high as 15 million.[32] There were five different versions of *Conficker*, all of which communicated via a peer-to-peer network of infected systems. The first four versions downloaded and installed what amounted to "self-preservation" updates that remained practically dormant. *Conficker E* (version 5) was the first to carry an actual payload of spam and "scareware" intended for outward execution.[33] The most important component of *Conficker* was not the worm itself, but the actual payload. The scareware warned of computer infection and requested credit card information to download an anti-virus fix. Unfortunately, the anti-virus was useless; the computer remained infected with *Conficker* and was subsequently susceptible to future exploitation.

The final pure form of malware is the Trojan horse (Trojan). "A Trojan horse is a malicious program that pretends to be a benign application. It purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive."[34] Trojans bait the end-user by posing as some recognized or legitimate program. This deception leads the user to execute the malignant script. While seemingly not as harmful as viruses, Trojans capture sensitive information and often leave backdoor access into a system for later use. Trojans are stealth in nature, which poses significant detection problems. Adversaries may repeatedly exploit systems infected with Trojans because the systems will often exhibit no signs of malfunction.

Since viruses, worms and Trojan horses each have unique strengths and weaknesses, many cyber adversaries use all three types of malware to construct blended threats. These blended threats combine the strengths of different types of malware in an effort to mitigate the individual weaknesses. In 2001, *Code Red* and *Nimda* became the first two widely-known blended threats. While the specific details of the two are beyond the scope of this paper, it is important to note that these threats were revolutionary; they solidified the notion that "single point solutions" were no longer valid for addressing malware. According to cyber security company Symantec, it became imperative to "protect all parts of the network and to respond on the Gateway, Server, and Client levels."[35] Furthermore, the number of systems affected, rate of infection, cost of lost productivity, and cost to remedy infections reached record levels. In fact, global costs reached an estimated $2.6B and $531M for *Code Red* and *Nimda*, respectively.[36]

In addition to other more sophisticated tools, adversary cyber actors use the aforementioned malware threats to enable bot networks or botnets (see Appendix A for a description of five common botnets). Subsequently, botnets are capable of enabling DoS attacks. A botnet is "a network of hijacked zombie computers controlled remotely by a hacker. The hacker uses the network to send spam and launch DoS attacks." [37] Botnets, also known as the "Swiss army knife" because of their versatility, are lethal in employing varied payloads. *Conficker*, which is technically a worm, effectively enabled a botnet since the "zombie" computers could be controlled remotely. At will, DoS attacks could have been launched via the infected network. A DoS attack is "an attack specifically designed to prevent the normal functioning of a system and thereby to prevent lawful access to the system by authorized users. Hackers can cause DoS attacks by destroying or modifying data or by overloading the system

servers until service to authorized users is delayed or prevented."[38] The effects of these attacks can be far reaching depending upon the sites targeted as well as the subject's capacity to respond.

Capability Implications

Clearly, even the most basic cyber tools have the ability to disrupt government networks. Many recent examples attest this fact. During the November 2005 cyber attack on the U.S. codenamed *Titan Rain*, attackers downloaded 10-20 terabytes of information from multiple unclassified DOD networks.[39] The specifics (tactics and tools) of this attack have not been made public. However, it can be assumed that some form of malware played a role in either the exploitation that led to the attack or the attack itself. In another instance, the *Conficker* worm was responsible for grounding French Naval fighter jets because it infected mission-planning databases.[40] In two more cases, hackers employed botnets and DoS attacks, among other tools, in the well-documented 2007 cyber attacks on Estonia and 2008 cyber attacks on Georgia. The Georgia attack was significant because it was the first occasion in which widespread cyber warfare was employed in conjunction with military force. The aforementioned examples represent only a few of the more highly publicized attacks. Unfortunately, everyday cyber actors are finding new and revolutionary methods for infiltrating networks and exploiting vulnerabilities.[41]

While the capabilities discussed above do not reference U.S. tactics specifically, they should drive the operator or mission planner to think about cyber operations in terms of desired effects. As opposed to thinking of purely kinetic solutions to targeting problems, CAF operators and planners must also bring non-kinetic options into the crosscheck. The desired effect should be the primary consideration when determining which option is best.

Section 5: Challenges

The numerous challenges that beset the cyber community at large are indeed complex, unique, and pervasive. This section, however, will narrow the scope to those challenges that pertain specifically to CNO and provide analysis in the areas of doctrine, organizational thought and system architecture, education and training, and planning. While it is not imperative that the CAF operator be well versed in the problems of cyber operations, it does behoove the CAF operator to have a baseline understanding of some of the key limitations that hamper community effectiveness.

Doctrine

The first and arguably most important problem area for CNO is doctrine. The capstone unclassified document for cyberspace, the National Military Strategy for Cyberspace Operations (NMS-CO), was released in 2006. Considering the current administration's focus on cyberspace and the planned establishment of USCYBERCOM, the NMS-CO must be revised. When addressing the country's new approach to cyber, the administration's 2009 Cyberspace Policy Review makes the following assertion.

> This approach requires clarifying the cybersecurity-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions. While efforts over the past two years started key programs and made great strides by bridging previously disparate agency missions, they provide an incomplete solution. Moreover, this issue transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective or authority to match the sweep of the problem.[42]

There are new directives and programs that are integral to cyberspace superiority. Clearly, the former status quo is no longer acceptable. While the NMS-CO still contains factually accurate

information, a revision is necessary to align with the most recent QDR, National Security Strategy, and directives of the President, as implemented by White House Cyber Coordinator.

One level below the NMS-CO lies joint cyberspace doctrine. Unfortunately, the joint publication that relates specifically to cyberspace operations does not yet exist. There is substantial discussion of CNO in JP 3-13. However, that publication does not provide the detail necessary to properly address CNO. All of the pillars of IO, with the exception of CNO, have separate publications. Although the joint publication status site does not indicate it, Joint Test Publication 3-12 *Cyberspace Operations* is currently in development.[43] Additionally, JP 6-01 *Electro-Magnetic Spectrum Operations* is under development and may have a CNO section embedded.[44] At present, no information is available on the layout of that publication. The resultant problem is that services are left to their own devices with the development of service doctrines, which ultimately hinders joint employment.

The USAF is leading the charge with the development of cyberspace doctrine. Air Force Doctrine Document (AFDD) 3-12 *Cyberspace Operations* is in draft form and due to go final in June or July 2010. This publication makes great strides in outlining the Air Force perspective for cyberspace operations. It incorporates the previously mentioned outdated strategic guidance as well as newer elements, such as USCYBERCOM. There is also a useful layout that details organizational responsibilities of the key players within the community.[45] The major challenge that is inherent in the draft surrounds its overall intent: The document states, "[t]he development of this doctrine document is intended to influence the creation of corresponding joint and allied doctrine."[46] The problem therein is the "watered-down" attempt to be too many things to too many organizations. In the absence of the joint publication, the AFDD endeavors to fill both roles. If the joint publication existed, however, it would provide the necessary foundation for the

AFDD and preclude the wide-ranging and aggressively academic prose in the current draft. Subsequently the AFDD could focus on its true intended purpose of informing USAF operations.

Organizational Thought and System Architecture

The challenges presented by organizational thought and system architecture are closely related. One NSA cyber operator, who spoke on condition of anonymity, suggested that organizational thought was a significant challenge to current cyber operations. In his estimate, "every service views CNO differently."[47] Ironically, it is this type of "organizational thought" that has led to significantly disparate system architecture and CNO capabilities within each service. A PACOM cyber expert agreed that each service meets the GCC requirements, but they do so in a slightly different manner. He cited multiple disparate architectures as significant because of the problems presented when requesting support from JFCC-NW and JTF-GNO. Furthermore the PACOM expert stated, "sourcing manpower for a specific requirement is difficult because, depending upon how specific (the requirement), you may be only able to use like-service guys to assist because only they understand the system."[48] With the limited number of cyber operators available, service-based restrictions further hamper efforts to support the warfighter. In a perfect cyber world, any cyber operator would be equally qualified to work on the system of any service. Granted, there is a certain level of defense in-depth built into a disparate architecture. However, does that added defense warrant the challenges presented in other areas such as elevated maintenance costs, separate training courses, separate acquisition requirements, and the like? Moreover, with the recent move toward joint basing, common system architecture is likely to become the norm. Presumably, one of the major advantages of the establishment of USCYBERCOM is that cyber operations will have a full-time advocate to

articulate the need for common architecture as well as joint standards that cover the full joint information environment.[49]

Education and Training

There are numerous publications that delve into the subject of cyber education and training. While education and training are often used interchangeably, a very important distinction separates the two. Dr Kamal Jabbour, from the Air Force Research Laboratory, provides the most succinct summation of that distinction when he remarks, "Training provides Airmen with proficiency to operate current tools, whereas education builds a foundation that prepares officers to deal with uncertain future challenges."[50] Obviously, both education and training are requirements to achieve cyberspace superiority; however, the challenge lies in the ability to strike the right balance between the types and quantities of education and training to produce the ultimate cyber scholar-warrior.

Officer advanced education

Before addressing advanced education, it is important to identify another significant challenge that is largely fundamental to force development. That challenge is the problem of attracting qualified applicants to enter the cyber career field. CNO requires a strong background in math and science. Logically, degrees that best establish the proper foundation for success in CNO include, but are not limited to, electrical engineering, computer engineering, computer science and physics. According to Defense Advanced Research Projects Agency (DARPA), "[t]he United States has entered into a significant national decline in the number of college graduates with science technology, engineering, and math (STEM) degrees."[51] Additionally, DARPA contends that, between 2003 and 2007, there was a 43% and 45% drop in computer science graduation and enrollment rates, respectively.[52] Therefore, it is not surprising that the Air

Force has also experienced a significant reduction in the number of STEM degreed officers. With a smaller base from which to recruit applicants, the cyber career field will experience difficulty growing its force. While there are many suggestions on ways to rectify this reduction in numbers, Dr. Jabbour offers one of the more interesting ones. He recommends adding an engineering degree prerequisite for entry into Undergraduate Pilot Training (UPT).[53] While execution of this recommendation would likely achieve the goal of a larger officer engineer base and subsequent cyber force, the undesirable third-order effect is a probable reduction in the number of qualified pilot training applicants which would lead to an undesired pilot shortage. Creating a deficiency in one career field is not the proper solution for rectifying a deficiency within another.

With regard to developing the current cyber force, in 2007, the USAF Scientific Advisory Board identified the fact that the Air Force provides "a lot more training and far less education" to its cyber warriors.[54] The resultant cyber force is extremely competent and proficient against known threats operating in a predictable manner; however, the force likely lacks the flexibility required to counter an unpredictable pop-up threat or near-peer adversary in today's dynamic environment. It is no secret that China is currently continuing significant strides toward the development of its information warfare force, specifically its computer confrontation operations capability. The massive Chinese training and educational effort has been ongoing since the mid-1990s.[55] The Chinese are convinced that their method of development will not only benefit the tactician in wartime operations but also the commander in matters of strategy and organization.[56]

The domestic challenge remains, still, to provide the cyber officer corps with more education in order to achieve the proper balance and maximize force potential. Accompanying the Air Force Institute of Technology (AFIT) IDE cyber warfare (ICW) program, several other

educational programs are in development. Appendix B shows the proposed cyber officer development path. In addition to the normal professional military education (PME), the cyber officer will also be required to accomplish professional continuing education (PCE). The PCE proposal includes Cyber 200, a 3-week in-residence course to be accomplished between the 6-8 year career mark and Cyber 300, a 2-week in-residence course to be accomplished between the 12-14 year career mark.[57] Both programs have a scheduled completion of October 2010.[58] Moreover, the Air Education and Training Command Commander tasked Air University (AU) to develop an Air Command and Staff College (ACSC) program that is additive to the ACSC curriculum with the goal of producing a cross-domain operator capable of integrating cyberspace effects at the operational level.[59] This program is scheduled for implementation during the 2011 academic year. While it appears as though education is on its way to achieving parity with training; funding, curriculum development, cadre selection, and permanent basing all may provide critical roadblocks that delay the cyber warrior-scholar reality.

Cross -domain integration (X-DI)

While the technical execution aspect of training is reportedly sufficient and improving, the foundational challenge in the training realm is to "spread the cyber word" across the other domains, specifically across the air domain. In order for cyber to have synergistic effects across the range of military operations (ROMO), all operators, specifically mission planners, must be cognizant of the capabilities of CNO, as well as understand how to effectively integrate them. That is why X-DI is important. Moreover, China is currently very active in X-DI. Every year, the Chinese accomplish hundreds of cyber exercises that touch "nearly every branch of service."[60] All indications are that information warfare will be an "integral part of the Chinese training plan for the foreseeable future."[61]

Since 2005, the United States Air Force Warfare Center (USAFWC) has led the charge for X-DI within the CAF. The USAF Weapons School (USAFWS) curriculum and Mission Employment (ME) Phase, Red Flag and Virtual Flag all currently have elements of CNO embedded. In fact, Red Flag 10-3 was the first to incorporate a non-kinetic package commander in the exercise.[62] The result is that mission commanders are now eager to synthesize non-kinetics from suppression of enemy air defenses and offensive counterair to dynamic targeting and special operations force missions. To date, the integration effort has been so successful that Pacific Air Forces (PACAF) made IO a Red Flag Alaska requirement.[63] This training is beneficial to all parties involved. In conjunction with providing CNO exercise support, the 67 NWW units also pursue their own learning objectives. Plans are in the works to expand CNO target sets and to incorporate Net-D training. These unprecedented efforts illuminate the importance placed upon X-DI by senior leadership as executed by the USAFWC.

Whereas "spreading the cyber word" is the fundamental challenge, there are two specific areas within that umbrella that plague X-DI. The first is time. Even though the USAFWS has reached key milestones in its endeavor to produce a "new generation of weapons officers who know no other way except for integrating non-kinetics", the resultant information trickle-down will take years to propagate throughout the CAF.[64] Flag exercises will increase CAF exposure and subsequently help to speed the process; however, more must be done in order to deliver the CNO message to the masses within a respectable time frame. The second and debatably more critical area is security classification levels. The USAFWC indicates that the cyber community is doing a great deal to declassify as much information as possible concerning effects and methods for integration.[65] While these steps are promising, the security levels of the actual capabilities could still present substantial difficulties likely resulting in devolvement to stove-piped mission

planning. Additionally, many of our sister-service personnel lack even the baseline clearances to discuss some of the more modest capabilities.[66] One would hope that joint campaign mission planners would receive the appropriate clearances prior to commencing planning. However, the desire is to integrate these capabilities during unit training which will in turn facilitate better execution and more wartime synergy. Furthermore, the declassification effort will take an abundance of time in addition to perseverance from leaders and operators alike.

Planning

With regard to planning, there are many deep-rooted challenges that the cyber operator must overcome. This section will focus on a few of the more pertinent challenges that affect the cyber operators' ability to support the combatant commander (CCDR). The discussion primarily surrounds the CNO subcomponents of CNA and CNE. While CCDRs have some capability resident within their theaters, a great deal of CNO expertise currently resides with JFCC-NW and JTF-GNO. Thus, it follows that the first planning challenge is to "get the right person in the right room". There are two aspects of this challenge that warrant mention. The first aspect is the acquisition of the requisite external support –"getting the right person". Whereas all CCDRs require a level of external support from JFCC-NW and JTF-GNO to assist in campaign planning, some theaters are relatively self-sufficient while others are heavily reliant. The support manifests itself in various forms to include intelligence support, planning conferences, and other special requests.[67] Getting support is no easy task based on current manning within the cyber career field. Furthermore, daily real-world operations also draw resources from these limited assets. However, when CCDR's are able to get the necessary planning support, the situational awareness and expertise resident within the JFCC-NW and JTF-GNO help the CCDRs' joint planning group (JPG) to produce a better product.

The second aspect of this challenge deals with the location of the CNO expertise during planning – "the right room". Whether contingency planning or crisis action planning, the IO cell is responsible for coordinating the planning of all CNO within an AOR. The IO cell is tasked to "integrate and synchronize the core capabilities of IO with IO-supporting and related capabilities and appropriate staff functions."[68] Although organization of the JPG varies dependent upon task, timing and commander preference, the IO cell is typically an integral JPG subcomponent. (See Appendix C for notional JPG and IO cell constructs.) The IO cell representative to the JPG is critical to ensuring IO integration and synchronization. Ideally, the representative to the JPG should be "well versed not only in IO planning but also in joint planning."[69] More importantly, the IO cell's JPG representative is the coordination linchpin. Therefore, the representative will likely spend more time managing the coordination of the more well known IO capabilities such as EW and PSYOP. It is not probable that the representative will have to time to "sell" the benefits of CNO integration, which may be necessary given that the average CAF operator knows very little about CNO and may not request it. The challenge is to force the actual CNO experts, the best advocates, to interact with the functional components and other JPG planners in order to publicize their capabilities. When the "right people", well versed in CNO capabilities, reach the "right room", the potential benefits of CNO will begin to be maximized at the operational level. Certainly, this particular challenge is more of a factor in some theaters than others – primarily due to the different capabilities, organizations and proficiencies resident. However, this challenge remains a perpetual one that will demand attention for some time to come.

The next planning challenge is the previously mentioned robust intelligence requirement. Not only does successful CNA require vast amounts of intelligence, CNA requires vast amounts

of frequently updated, correct intelligence. In the capabilities section, we discussed how networks must be mapped in order to be properly and stealthily infiltrated. When tools are developed, they are typically built for a specific network at a specific point in time. Changes such as software, hardware, and security updates can all render a tool obsolete. In the absence of current, accurate supporting intelligence to verify the status of target networks, it is highly likely that attacks will be ineffective, best case, and detected, worst case. When discussing his approach to CNA intelligence requirements, one PACOM cyber expert stated, ”My first question is what is the date/time group on this information that you are giving me? When was it last checked? If it was last week, then it may as well have been last year. If it was yesterday, then maybe we are within the realm of possibility…but even that is going to be suspect.”[70]

This challenge manifests differently depending upon whether it is relative to crisis-action planning or contingency planning. In the midst of crisis-action planning, time is often the single most limiting factor. It takes time to gather the intelligence, develop the tool, test the tool, re-verify the intelligence, and execute. Dependent upon the period it takes to accomplish these required tasks, the need for the tool may no longer exist. During contingency planning, capabilities are developed for systems as currently configured. Those capabilities are then shelved, only to be executed when circumstances dictate. While the tools will be updated with subsequent plan revisions, there could be significant system changes between the final update and plan execution. The intelligence requirement is paramount during each plan revision. Furthermore, since no plan is executed “off the shelf”, there will be some version of crisis action planning, which in turn requires intelligence support Ultimately, it becomes a matter of using vast amounts of intelligence to develop a new tool over a short period or revising an old tool over

a slightly longer period. Either way, filling the robust intelligence requirement in a timely manner is the challenge.

The final planning challenge is the coordination across AORs and agencies. This responsibility falls upon USSTRATCOM. Based on the global nature of the internet and networks, coordination can be quite challenging. It is never clear which agency may be exploiting a particular node that warrants targeting within a campaign plan. Due to the lack of physical borders within cyberspace, actions in one AOR can have global effects in a matter of seconds. In fact, according to direction in the 2003 Secretary of Defenses' Information Operations Roadmap, CNA weapons are categorized based on release authority. Category I weapons are releasable by the Combatant Commander; Category II weapons are pre-allocated to support a specific aspect of an operational plan or contingency plan; Category III weapons require President/SECDEF approval.[71] However, due to high potential for collateral damage through unintended third and fourth order effects, all CNA targets must still be deconflicted throughout the services, as well as the intelligence community.[72] Depending upon the scope, this process can be lengthy and result in a missed opportunity with respect to CNO.

Section 6: Recommendations and Future Research

Doctrine

In addition to updating the NMS-CO, the production of JP-3-12 Cyberspace Operations must be accelerated. With the impending activation of USCYBERCOM, the absence of a joint publication makes the colossal tasks of standardization across services that much more difficult. Considering the fact that each service is in the process of standing up its own cyber component, JP 3-12 needs to devote significant text to approved methods for cross-service cooperation and cross-domain integration as well as a detailed section on possible means for better CNO

integration within the IO cell and within the JPG. One factor that may hinder the acceleration of JP 3-12 is the ongoing rewrite of JP 3-13. Multiple sources indicate significant changes are in the works for JP 3-13. Obviously, restructuring the IO parent document could have wide-spread affect on the upcoming JP 3-12. The sources also agree that there will be "no movement" on JP 3-12 until JP 3-13 is complete.[73,74] Nevertheless, CNO integration in joint operations will be limited until the JP 3-12 is released.

When addressing Air Force doctrine, AFDD 1 *Air Force Basic Doctrine* states, "these publications express why air and space power is different from other forms of military power, how it should be organized and employed, and why it's best to do things certain ways."[75] Furthermore, it states that, "Doctrine explains why certain organizational structures are preferred over others and describes effective command relationships and command authorities."[76] Considering that cyberspace superiority is a core Air Force function and winning in cyberspace is a key component of the Air Force mission statement, the final version of AFDD 3-12 should devote some text to addressing why the Air Force is best suited for the task of cyberspace superiority. While air and space superiority clearly fall within the purview of the Air Force, cyberspace superiority is not an obvious fit. Although the USAF currently is leading the charge, simple initiative does not necessarily imply accuracy in judgment or rightful ownership. There is no better place to make the case for ownership than AFDD 3-12.

Organizational Thought and System Architecture

The only pertinent recommendation for this section is actually an area for future research. As previously mentioned, due to reductions in funding, the activation of USCYBERCOM, and the introduction of joint basing throughout DOD; the issue of standardized architecture is no longer a question of "if", but more a question of "when". It follows then that once the services

are standardized, there may no longer be a requirement for separate service training. If this proves true, maybe training will migrate to a cross-service program much like present-day water survival, airborne school and the upcoming F-35 course. If research results favor joint training, then where will it be located? How will it be structured? Who will operate it? Due to the probable discussion of specific training requirements, this research will likely be classified.

Education, Training and Planning

There is one recommendation that would make strides toward the goal of educating cyber leaders. In his *Air and Space Power Journal* article, Major Paul William recommends creation of a cyber advanced studies track that would mirror the current School of Advanced Air and Space Studies (SAASS) program. He states that sending select ACSC graduates to AFIT for the ICW course as a method for producing officers who are able to "generate innovative thought needed to develop cyber power as a war-fighting function…[and] become respected and influential leaders of the cyberspace forces."[77] This recommendation makes sense considering the current state of the cyber force and the need to rapidly develop future leaders. However, the recommendation will only be useful to fill the current gap. Once the lieutenants of today reach IDE, it is probable that they will already possess advanced cyber degrees and will benefit the service more by attending SAASS or a sister-service equivalent.

When conducting the research for this paper, the following question was repeatedly asked of each cyber expert: "*What does the CAF operator or mission planner need to know about cyber?"* Time and again, the responses were similar: *Tell us (cyber operators) what effect you want and we will make it happen*. The author determines that this answer is only half of the solution. There is more to true X-DI than CAF operators and mission planners simply ordering from an "effects menu" and waiting for delivery. The other side of the equation is for the true

cyber experts to take a seat at the mission planning table and collaboratively solve operation/tactical problems. This is the culture shift currently being advocated by the USAFWC.[78] Additionally, the USAFWS Cyber Weapons Instructor Course (WIC), once established, will promote that same mentality among cyber operators as well as facilitate reciprocity from the CAF. When cyber capabilities become the standard operations for USAFWS operations, integration of CNO in the campaign planning will then be second nature. Until this happens however, the USAF must take steps towards normalizing this nascent culture shift throughout the CAF and ensuring that momentum is not lost.

Concerning future research in the education, training and planning realm, a classified version of this document that details relevant friendly capabilities and available effects would be vital to the CAF understanding of CNO. Ultimately, the document could serve as a pseudo-CNO playbook for the CAF. It should provide basic effects as a point of departure for mission planning discussions. There is no requirement for the document to be overly technical. Most CAF operators will simply want to know what effects are possible, not necessarily, how they are accomplished.

Section 7: Conclusion

The Air Force is making great strides in its effort to win in cyberspace. The goal of this project was to further that mission by outlining the essential information required for the CAF operator to ensure working knowledge of CNO, thus facilitating more efficient, synergistic integration into the warfighting structure.

Section 1 provided the framework for the discussion by defining cyberspace and detailing its pervasive nature. Additionally, section 1 provided key background information regarding current United States Government strategic views and DOD views on cyberspace. This

information helped to illuminate the sound logic behind the significance placed on securing the nation's heavily relied upon networks.

Section 2 began the CNO education by showing where CNO fits into the overarching information operations construct. Subsequently, CNO was dissected in order to adequately explain the fundamental elements of CNA, CNE and CND. Section 2 concluded with a generic discussion of the interaction between each of the elements.

Section 3 furthered the discussion by detailing how cyber forces are organized. The section started with an introduction of USSTRATCOM, the lead DOD agency, and worked in a top-down manner all the way through USAF CNO assets. Section 3 concluded with a brief explanation of USCYBERCOM and its potential for success.

Section 4 outlined the importance of cyberspace, specifically CNO, to the warfighter. The first half of this section covered vulnerabilities as well as potential implications if those vulnerabilities are compromised. Due to the classification of U.S. specific capabilities, the second half of section 4 gave an overview of generic exploitation and attack tools currently employed by cyber players. The last portion of section 4 delivered analysis on implications of employing specific tools in order to drive the CAF mission planner or operator to think in terms of desired effects.

Section 5 highlighted a few of the key operational challenges that beset CNO. Analysis was limited to the areas of doctrine, organizational thought and system architecture, education and training, and planning. This discussion was intended to provide the CAF operator with a high level understanding of the unique nature of the challenges faced by cyber operators. The goal was to lend insight to issues that may hamper CNO support to the warfighter.

Finally, section 6 concluded the discussion by offering recommendations in the same areas discussed in section 5 in order to achieve the goal of more efficient joint cross-domain operations. Additionally, section 6 detailed several recommendations for future research in the hopes of furthering the necessary CAF operator-CNO operator dialogue.

Many scholars believe that the first battle of future wars against any technologically savvy opponent will take place in and through cyberspace.[79] If their theories prove true, the battle for cyber dominance will require skillful integration of cyberspace capabilities across every aspect of our current warfighting structure. To achieve that integration, it is paramount that the CAF make a major effort to increase its knowledge base in order to facilitate smooth transition. Through the discussion of CNO – its organization, its importance, and its challenges – this research makes the first small step.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Appendix A America's Five Most Wanted Botnets[80]

Botnet attacks are increasing, as cybercrime gangs use compromised computers to send spam, steal personal data, perpetrate click fraud and clobber Web sites in denial-of-service attacks. Here's a list of America's 5 most wanted botnets, based on an estimate by security firm Damballa of botnet size and activity in the United States:

1. Zeus - Compromised US computers: 3.6 million.
The Zeus Trojan uses key-logging techniques to steal sensitive data such as user names, passwords, account numbers and credit card numbers. It injects fake HTML forms into online banking login pages to steal user data.

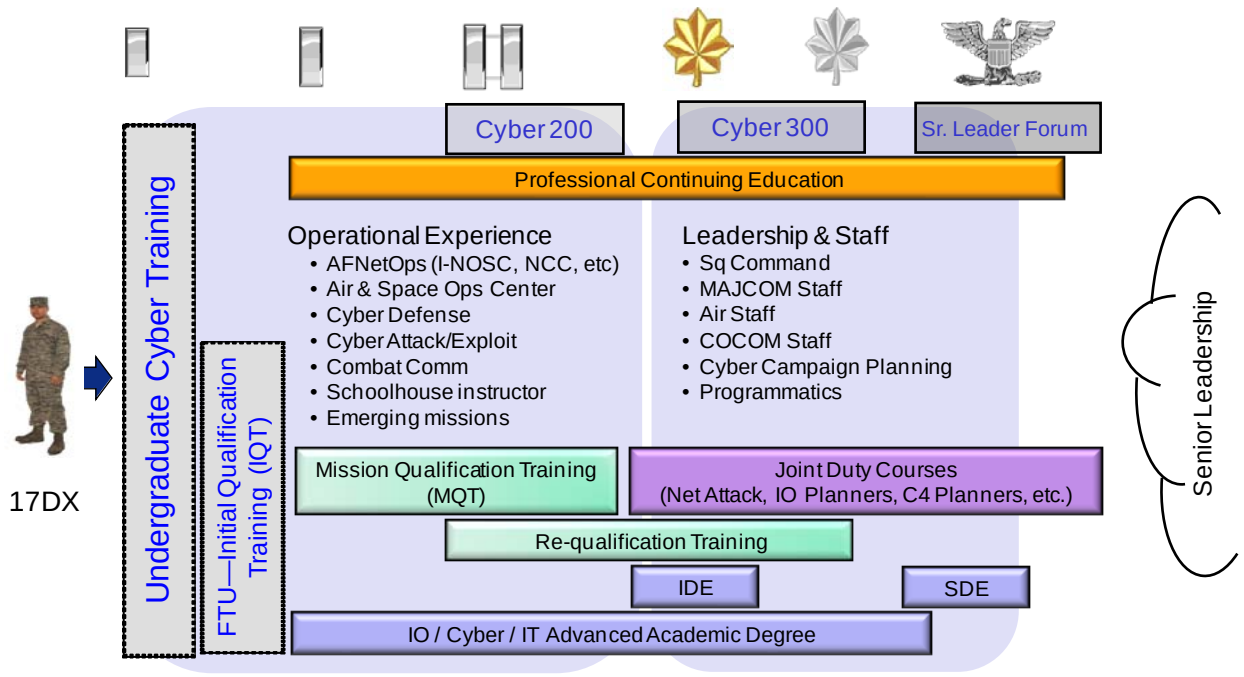
2. Koobface - Compromised US computers: 2.9 million.
This malware spreads via social networking sites MySpace and Facebook with faked messages or comments from "friends." When a user is enticed into clicking on a provided link to view a video, the user is prompted to obtain a necessary update, like a codec -- but it's really malware that can take control over the computer.

3. TidServ - Compromised US computers: 1.5 million.
This downloader Trojan spreads through spam e-mail, arriving as an attachment. It uses rootkit techniques to run inside common Windows services (sometimes bundled with fake antivirus software) or in Windows safe mode, and it can hide most of its files and registry entries.

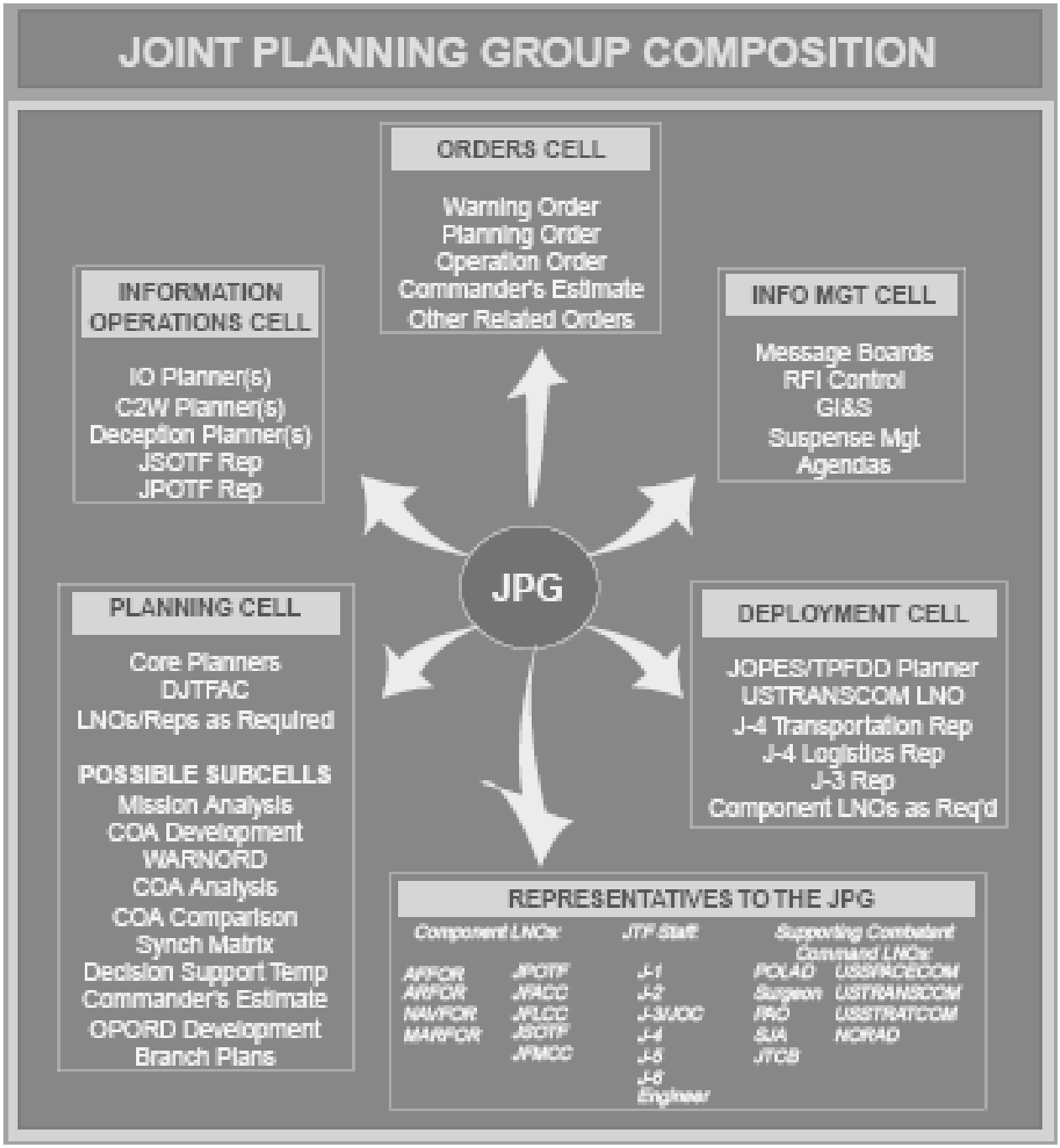
4. Trojan.Fakeavalert - Compromised US computers: 1.4 million.
Formerly used for spamming, this botnet has shifted to downloading other malware, with its main focus on fake alerts and rogue antivirus software.

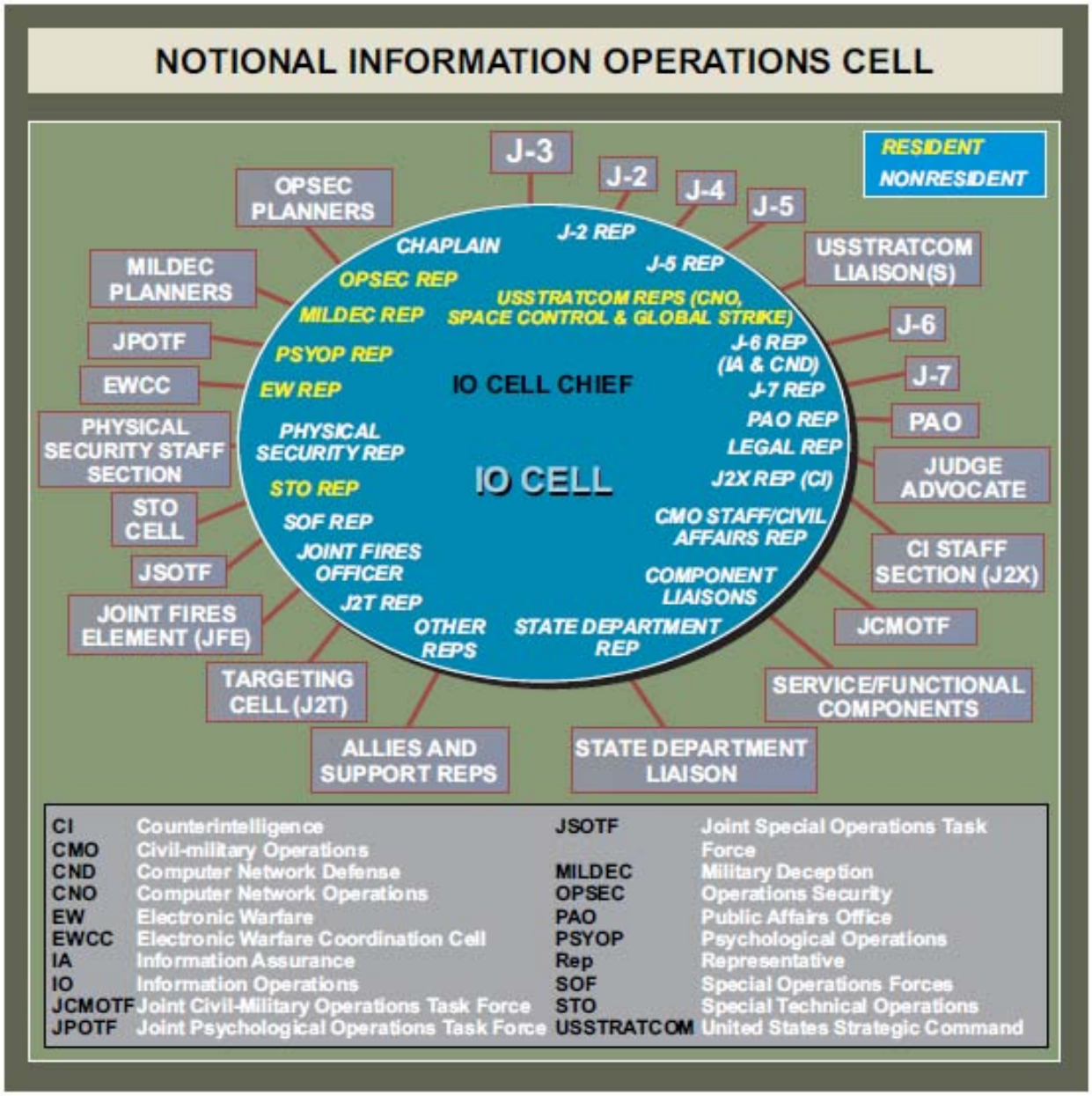
5. TR/Dldr.Agent.JKH - Compromised U.S. computers: 1.2 million.
This remote Trojan posts encrypted data back to its command-and-control domains and periodically receives instruction. Often loaded by other malware, TR/Dldr.Agent.JKH is currently used as a clickbot, generating advertisement revenue for the botmaster through constant advertisement-specific activity.

Appendix B Proposed USAF Cyberspace Officer Development[81]



Appendix C Notional JPG and IO Cell Composition[82,83]




NOTIONAL INFORMATION OPERATIONS CELL
RESIDENT
NONRESIDENT
J-3
J-2
J-4
J-5
J-6
J-7
OPSEC PLANNERS
MILDEC PLANNERS
JPOTF
EWCC
PHYSICAL SECURITY STAFF SECTION
STO CELL
JSOTF
JOINT FIRES ELEMENT (JFE)
TARGETING CELL (J2T)
ALLIES AND SUPPORT REPS
STATE DEPARTMENT LIAISON
SERVICE/FUNCTIONAL COMPONENTS
JCMOTF
CI STAFF SECTION (J2X)
JUDGE ADVOCATE
PAO
USSTRATCOM LIAISON(S)
CHAPLAIN
OPSEC REP
MILDEC REP
PSYOP REP
EW REP
PHYSICAL SECURITY REP
STO REP
SOF REP
JOINT FIRES OFFICER
J2T REP
OTHER REPS
J-2 REP
J-5 REP
USSTRATCOM REPS (CNO, SPACE CONTROL & GLOBAL STRIKE)
J-6 REP (IA & CND)
J-7 REP
PAO REP
LEGAL REP
J2X REP (CI)
CMO STAFF/CIVIL AFFAIRS REP
COMPONENT LIAISONS
STATE DEPARTMENT REP
IO CELL CHIEF
IO CELL
CI Counterintelligence
CMO Civil-military Operations
CND Computer Network Defense
CNO Computer Network Operations
EW Electronic Warfare
EWCC Electronic Warfare Coordination Cell
IA Information Assurance
IO Information Operations
JCMOTF Joint Civil-Military Operations Task Force
JPOTF Joint Psychological Operations Task Force
JSOTF Joint Special Operations Task Force
MILDEC Military Deception
OPSEC Operations Security
PAO Public Affairs Office
PSYOP Psychological Operations
Rep Representative
SOF Special Operations Forces
STO Special Technical Operations
USSTRATCOM United States Strategic Command

Endnotes

[1] Daniel T. Kuehl, "From Cyberspace to Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington, DC: Potomac Books Inc, 2009), 28.
[2] The Office of the President, *The White House*, *The National Strategy to Secure Cyberspace*, (Washington, DC: Office of the President, 2003), vii.
[3] Barack H. Obama, *Remarks by the President on Securing our Nation's Cyber Infrastructure*, (Washington, DC: Office of the Press Secretary, 29 May 2009).
[4] US Department of Defense, *Quadrennial Defense Review Report*, (Washington, DC: Department of Defense, February 2010), 37.
[5] Ibid.
[6] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (as Amended through 31 October 2009), 227.
[7] US Department of Defense Instruction (DODI) 8410.02, *NetOps for the Global Information Grid (GIG)*, 19 December 2008. 11.
[8] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, GL-9.
[9] Ibid, II-5.
[10] Ibid.
[11] Leigh Armistead, *Information Operations*, (Washington, DC, Brassey's Inc, 2004), 116.
[12] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, II-5.
[13] United States Air Force Space Command, *Concept of Operations for Twenty Fourth Air Force Cyberspace Operations*, 30 March 2009, 11.
[14] United States Air Force Scientific Advisory Board, *Report on Implications.of Cyberwarfare Volume 1*, August 2007, 23.
[15] US Department of Defense, *Unified Command Plan*, December 2008.
[16] USSTRATCOM official website, http://www.stratcom.mil/functional_components/ (accessed 1 January 2010).
[17] Ibid.
[18] United States Air Force Space Command, *Concept of Operations for Twenty Fourth Air Force Cyberspace Operations*, 30 March 2009, 10.
[19] Ibid, 19.
[20] Secretary of Defense to Secretaries of the Military Departments, et al, Memorandum for Establishment of a Subordinate Unified U.S. Cyber Command under US Strategic Command for Military Cyberspace Operations, 23 June 2009.
[21]Gerri J. Gilmore, "Lynn Lists Aerospace, Cyber-age Challenges," *AF.mil*, 22 January 2010, http://www.af.mil/news/story.asp?id=123186689 (accessed 1 March 2010).
[22] Gen Kevin P. Chilton, commander US Strategic Command, (address Air Force Association 2009 Global Warfare Symposium, Los Angeles, CA, 20 November 2009).
[23] SysAdmin, Audit, Network, Security Institute, "Top security risks September 2009," *SANS.org*, http://www.sans.org/top-cyber-security-risks/#trends (accesed 12 March 2010).
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Dr. Daniel T. Kuehl, (Professor, National Defense University), interview by author, 19 February 2010
[28] Timothy P. Franz, "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way Ahead for Network Warfare Forces," (master's thesis, Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007).
[29] Mcafee Website, "Glossary," *Mcafee.com*, http://home.mcafee.com/virusinfo/Glossary.aspx (accessed 10 March 2010).
[30] SysAdmin, Audit, Network, Security Institute, "Intrusion Detection FAQ: What was the Melissa virus and what can we learn from it?" *SANS.org* http://www.sans.org/security-resources/idfaq/what_melissa_teaches_us.php (accessed 10 Mar ch 2010).
[31] Mcafee Website, "Glossary," *Mcafee.com*, http://home.mcafee.com/virusinfo/Glossary.aspx (accessed 10 March 2010).

[32] Ned Potter, "Conficker Computer Worm Threatens Chaos," *ABC.com*, 25 March 2009, http://abclocal.go.com/wpvi/story?section=news/technology&id=6728349 (accessed 10 March 2010).
[33] Elinor Mills, "Conficker Infected Critical Hospital Equipment, expert says," *CNET.com*, 23 April 2009, http://news.cnet.com/8301-1009_3-10226448-83.html (accessed 10 March 2010).
[34] Mcafee Website, "Glossary", *Mcafee.com*, http://home.mcafee.com/virusinfo/Glossary.aspx (accessed 10 March 2010).
[35] Symantec, *Responding to the Nimda worm: Recommendations for Addressing Blended Threats*, 3 http://www.symantec.com/avcenter/reference/nimda.final.pdf (accessed 10 March 2010).
[36] Ibid.
[37] Mcafee Website, "Glossary", *Mcafee.com*, http://home.mcafee.com/virusinfo/Glossary.aspx (accessed 10 March 2010).
[38] Ibid.
[39] Dawn S. Onley, "Red Storm Rising," *GCN.com*, 17 August 2006, http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx?p=1 (accessed 11 March 2010).
[40] Kim Willsher, "French Fighter Planes Grounded by Computer Virus," *Telegraph.co.uk*, 7 February 2009, http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (accessed 11 March 2010).
[41] Fred Green (CISCO Systems Engineer, Network Security Specialist), interview by author, 11 March 2010.
[42] National Security Council and Homeland Security Council, *The Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure*, (Washington, DC: Government Printing Office, May 2009), iii.
[43] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations DRAFT v3d-7, 14.*
[44] Joint Electronic Library, *Joint Doctrine Heirarchy*, 17 February 2010, http://www.dtic.mil/doctrine/doctrine/status.pdf (accessed 18 March 2010).
[45] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations DRAFT v3d-7*, 19.
[46] Ibid 14.
[47] Interview with cyber expert from NSA, 24 February 2010.
[48] Interview with cyber expert from PACOM, 3 March 2010.
[49] Ibid.
[50] Dr. Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly* Volume 4 No 1, (Spring 2010), 71.
[51] Defense Advanced Research Projects Agency (DARPA) Information Processing Techniques Office (IPTO), *DARPA-RA-10-03 Computer Science - Science, Technology, Engineering, and Mathematics (CS-STEM) Education Research Announcement*, 12 January 2010, https://www.fbo.gov/download/69c/69c81b4b7f892d4e0e0d8a7bec0eba29/CS-STEM,_DARPA-RA-10-03,_12Jan10.pdf (accessed 1 April 2010).
[52] Ibid.
[53] Dr. Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly* Volume 4 No 1, (Spring 2010), 71.
[54] United States Air Force Scientific Advisory Board, *Report on Implications of Cyber Warfare Volume 2: Final Report SAB-TR-07-02*, August 2007, 39.
[55] Timothy L. Thomas, *Dragon Bytes, Chinese Information War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 18.
[56] Ibid, 22.
[57] Briefing, SAF/XCTF, subject: Comm & Info / Cyberspace Force Development, March 2010. https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=AF-SC-01-25-2&Filter=AF-SC-01-25 (accessed 18 March 2010).
[58] Minutes of the Cyber Professional Continuing Education (PCE) Cyber 200-300 Working Group, 22 March 2010 https://www.my.af.mil/afknprod/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-ED-IT-19-31-1&Filter=OO-ED-IT-19 (accessed 1 April 2010).
[59] Briefing, Air University, subject: Cross Domain Operator Course of Action Decision Brief, October 2009.
[60] Timothy L. Thomas, *Dragon Bytes, Chinese Information War Theory and Practice.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 63.
[61] Ibid, 64.
[62] Lt Col William H. Poe, (USAFWC/A3I), interview by author, 1 April 2010.

[63] Briefing, United States Air Force Warfare Center, subject: Cyber Integration in USAF Warfare Center Brief, 24 April 2009.
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Interview with cyber planner from USSTRATCOM, 22 February 2010.
[68] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, IV-4.
[69] Joint Forces Staff College, *Joint Information Operations Planning Handbook*, March 26, 2008, I-16.
[70] Interview with cyber expert from PACOM, 3 March 2010.
[71] US Department of Defense, *Information Operations Roadmap*, (Washington DC: Department of Defense 30 October 2003), 57.
[72] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, V-3
[73] Interview with CNO Planner from JFCC-NW, 12 March 2010.
[74] Dr. Daniel T. Kuehl, (Professor, National Defense University), interview by author, 19 February 2010.
[75] Air Force Doctrine Document (AFDD)1, *Air Force Basic Doctrine*, 17 November 2003, *2.*
[76] Ibid, *5*.
[77] Paul D. Williams, "Cyber ACTS/SAASS A Second Year of Command and Staff College for the Future leaders of Our Cyber Forces," *Air and Space Power Journal Volume* XXIII, No. 4, (Winter 2009):21-29.
[78] Lt Col William H. Poe, USAFWC/A3I, interview by author, 1 April 2010.
[79] Robert A. Miller and Kuehl, Daniel T. "Cyberspace and the "First Battle" in 21st Century War", *Defense Horizons Number 68*, September 2009, 2, http://www.ndu.edu/ctnsp/defense_horizons/DH68.pdf (accessed 2 February 2010).
[80] 624th Operation Center Intelligence Surveillance Reconnaissance Division Cyber Threat Bulletin, 19 March 2010 (Issue 48), https://www.my.af.mil/gcss-af/USAF/AFP40/d/sA1FBF31D23C34A850123C9CE6173015B/Files/Cyber%20Threat%20Bulletin%2019%20March%202010.pdf?channelPageId=s6925EC1356510FB5E044080020E329A9 (accessed 18 March 2010).
[81]Briefing, SAF/XCTF, subject: Force Development, Comm & Info / Cyberspace Force Development, March 2010. https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=AF-SC-01-25-2&Filter=AF-SC-01-25 (accessed 18 March 2010).
[82]Joint Forces Staff College, *Joint Information Operations Planning Handbook*, March 26, 2008, I-16.
[83] Joint Publication (JP) 3-13, *Information Operations*, 13 February 2006, IV-4.

Bibliography

624th Operation Center Intelligence Surveillance Reconnaissance Division. *Cyber Threat Bulletin*, 19 March 2010 (Issue 48). https://www.my.af.mil/gcss-af/USAF/AFP40/d/sA1FBF31D23C34A850123C9CE6173015B/Files/Cyber%20Threat%20Bulletin%2019%20March%202010.pdf?channelPageId=s6925EC1356510FB5E044080020E329A9

AF/A3O-CF. *The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2013*. Washington, DC, 2008.

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*, 17 November 2003.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, 11 January 2005.

Air Force Doctrine Document 3-12. *Cyberspace Operations DRAFT v3d-7*.

Air Force Institute of Technology (AFIT). Center for Cyberspace Research (CCR). http://www.afit.edu/ccr/ (accessed 2 January 2008).

Armistead, Leigh. *Information Operations*. Washington, DC: Brassey's Inc, 2004.

Briefing. Air University. Subject: Cross Domain Operator Course of Action Decision Brief, October 2009.

Briefing. SAF/XCTF. Subject: Comm & Info / Cyberspace Force Development, March 2010. https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=AF-SC-01-25-2&Filter=AF-SC-01-25 (accessed 18 March 2010).

Briefing. SAF/XCTF. Training Future Cyber Professionals, November 2009. https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=AF-SC-01-25-2&Filter=AF-SC-01-25 (accessed 18 March 2010).

Briefing. United States Air Force Warfare Center. Subject: Cyber Integration in USAF Warfare Center Brief, 24 April 2009.

Chilton, Gen Kevin P., commander US Strategic Command. Address. Air Force Association 2009 Global Warfare Symposium, Los Angeles, CA, 20 November 2009.

Courville, Shane P. "Air Force and the Cyberspace Mission: Defending the Air Forces's Computer Network in the Future." Research Paper, Air Command and Staff College, 2007.

Convertino II, Sebastian M., Lou A. DeMattei, and Tammy M. Knierim. "Flying and Fighting in Cyberspace." Air War College Maxwell Paper No. 40. Maxwell AFB, AL: Air War College, 2007.

Defense Advanced Research Projects Agency (DARPA) Information Processing Techniques Office (IPTO). *DARPA-RA-10-03 Computer Science - Science, Technology, Engineering, and Mathematics (CS-STEM) Education Research Announcement.* 12 January 2010 https://www.fbo.gov/download/69c/69c81b4b7f892d4e0e0d8a7bec0eba29/CS-STEM,_DARPA-RA-10-03,_12Jan10.pdf (accessed 1 April 2010).

Franz, Timothy P. "IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces." Master's thesis, Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007.

Gilmore, Gerri J. "Lynn Lists Aerospace, Cyber-age Challenges." *AF.mil*, 22 January 2010. http://www.af.mil/news/story.asp?id=123186689 (accessed 1 March 2010).

Grant, Rebecca. "Victory in Cyberspace." Air Force Association, 2007.

Halle, Ann M. *Cyberpower as a Coercive Instrument*. Master's thesis, Maxwell AFB, AL: The School of Advanced Air and Space Studies, 2009.

Headquarters United States Air Force. *Program Action Directive 07-08 Change 3*, 20 February 2009

Jabbour, Dr. Kamal T. "Cyber Vision and Cyber Force Development." *Strategic Studies Quarterly* Volume 4 No 1, (Spring 2010):63-73.

Jabbour, Dr. Kamal T. *"50 Cyber Questions Every Airman Can Answer."* Air Force Research Laboratory, 2008.

Joint Electronic Library. *Joint Doctrine Hierarchy*. 17 February 2010. http://www.dtic.mil/doctrine/doctrine/status.pdf (accessed 18 March 2010).

Joint Forces Staff College. *Joint Information Operations Planning Handbook.* March 26, 2008.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 12 April 2001 (as Amended through 31 Oct 2009).

Joint Publication (JP) 3-13. *Information Operations,* 13 February 2006.

Joint Publication (JP) 5-0. *Joint Operation Planning*, 26 December 2006.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24-42. Potomac Books, Inc., Washington DC, 2009.

Mcafee Website. "Glossary." *Mcafee.com*, http://home.mcafee.com/virusinfo/Glossary.aspx (accessed 10 March 2010).

Miller, Robert A and Daniel T. Kuehl. "Cyberspace and the "First Battle" in 21st Century War." *Defense Horizons* Number 68, September 2009. http://www.ndu.edu/ctnsp/defense_horizons/DH68.pdf (accessed 2 February 2010).

Mills, Elinor. "Conficker Infected Critical Hospital Equipment, expert says." *CNET.com*, 23 April 2009. http://news.cnet.com/8301-1009_3-10226448-83.html (accessed 10 March 2010).

Minutes. Cyber Professional Continuing Education (PCE) Cyber 200-300 Working Group, 22 March 2010. https://www.my.af.mil/afknprod/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-ED-IT-19-31-1&Filter=OO-ED-IT-19 (accessed 1 April 2010).

National Security Council and Homeland Security Council. *The Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: Government Printing Office, May 2009.

Obama, Barack H. *Remarks by the President on Securing our Nation's Cyber Infrastructure*. Washington, DC: The White House Office of the Press Secretary, 2009.

Onley, Dawn S. "Red Storm Rising." GCN.com, 17 August 2006. http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx?p=1 (accessed 11 March 2010).

Potter, Ned. "Conficker Computer Worm Threatens Chaos." *ABC.com*, 25 March 2009. http://abclocal.go.com/wpvi/story?section=news/technology&id=6728349 (accessed 10 March 2010).

Secretary of Defense to Secretaries of the Military Departments, et al. Memorandum for Establishment of a Subordinate Unified U.S. Cyber Command under US Strategic Command for Military Cyberspace Operations, 23 June 2009.

Symantec. *Responding to the Nimda worm: Recommendations for Addressing Blended Threat.* http://www.symantec.com/avcenter/reference/nimda.final.pdf (accessed 10 March 2010).

SysAdmin, Audit, Network, Security Institute. "Top security risks September 2009." *SANS.org*, http://www.sans.org/top-cyber-security-risks/#trends (accesed 12 March 2010).

SysAdmin, Audit, Network, Security Institute. "Intrusion Detection FAQ: What was the Melissa virus and what can we learn from it?" *SANS.org*, http://www.sans.org/security-resources/idfaq/what_melissa_teaches_us.php (accessed 10 March 2010).

The Office of the President. *The White House The National Strategy to Secure Cyberspace*. Washington, DC: Government Printing Office, 2003.

Thomas, Timothy L. *Dragon Bytes, Chinese Information War Theory and Practice.* Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

Thomas, Timothy L. "The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia." *The Journal of Slavic Military Affairs,*Volume 22, Issue 1 (January 2009):31-67.

United States Air Force Space Command. *Concept of Operations for Twenty Fourth Air Force Cyberspace Operations,* 30 March 2009.

United States Air Force Scientific Advisory Board. *Report on Implications.of Cyberwarfare Volume 1,* August 2007.

United States Air Force Scientific Advisory Board. *Report on Implications of Cyber Warfare Volume 2: Final Report SAB-TR-07-02,* August 2007.

US Cyber Consequences Unit. "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008." August 2009. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (accessed 25 February 2010)

US Department of Defense. *Information Operations Roadmap.* Washington DC: Department of Defense 30 October 2003.

US Department of Defense Instruction (DODI) 8410.02. *NetOps for the Global Information Grid (GIG),* 19 December 2008.

US Department of Defense. *National Military Strategy for Cyberspace Operations*. Washington DC: Department of Defense, May 2006.

US Department of Defense. *Quadrennial Defense Review Report.* Washington, DC: Department of Defense, February 2010.

US Department of Defense. *Unified Command Plan*, December 2008.

US Strategic Command (USSTRATCOM) Official Website. http://www.stratcom.mil/functional_components/ (accessed 1 January 2010).

Williams, Paul D. "Cyber ACTS/SAASS A Second Year of Command and Staff College for the Future leaders of Our Cyber Forces." *Air and Space Power Journal* Volume XXIII, No. 4, (Winter 2009): 21-29.

Willsher, Kim. "French Fighter Planes Grounded by Computer Virus." *Telegraph.co.uk*, 7 February 2009. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (accessed 11 March 2010).

Wilson, Clay. "Information Operations and Cyberwar: Capabilities and Related Policy Issue." *Congressional Research Service Report for Congress.* Washington DC: The Library of Congress, 14 September 2006.